~~TOP SECRET~~

[redacted]

DCI/ICS 86-4043

6 March 1986

MEMORANDUM FOR: Acting Director of Central Intelligence

FROM: VADM E. A. Burkhalter, Jr., USN
Director, Intelligence Community Staff

SUBJECT: Congressional Query: Security Implications of Expanded Use of Computers and Word Processing Equipment

REFERENCE: Classified Annex to HAC Report on the FY86 DoD Appropriations Bill, dated 28 October 1985, [redacted] pp. 17 and 18 STAT

1. Action Requested: Your signature on the attached in response to the referenced request. [redacted] STAT

2. Background: The House Appropriations Committee (HAC) requested that a report be submitted by 1 March 1986 outlining the actions being taken by each Intelligence Community (IC) and Department of Defense (DoD) component to strengthen physical and electronic computer and automated office equipment security. The HPSCI and SAC have requested copies of the responses to this HAC tasking in lieu of establishing separate reporting requirements on this subject. [redacted] STAT

3. The focus of the HAC request is on security procedures that IC and DoD components have instituted to protect against the opportunities for disloyal employees to compromise or steal sensitive intelligence data available in the storage media of word processors and small computers. The HAC cites the Walker and other recent espionage cases as prompting its concern and requests that the report specifically address changes which may be needed in intra-office procedures to minimize security risks associated with transportable discs, tapes, etc., containing sensitive information. [redacted] STAT

[redacted] STAT

~~TOP SECRET~~

STAT

[redacted]

4. Staff Coordination: DoD requested that the ICS prepare a consolidated DCI-DoD response and provided input covering TIARA elements. [redacted] concurs in the proposed response. [redacted]

STAT

STAT

5. Recommendation: Your approval and signature on the attachment. [redacted]

STAT

[redacted]

STAT

E. A. Burkhalter, Jr.
Vice Admiral, USN

Attachment:
As stated

[redacted]

The Director of Central Intelligence

Washington, D.C. 20505

13 MAR 1986

The Honorable Joseph P. Addabbo, Chairman
Subcommittee on Defense
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

In response to your Subcommittee's concern regarding the security implications of expanded Intelligence Community use of computer and word processing equipment, I am providing you herewith a summary assessment of the security risks associated with using these devices, the mechanisms in place to protect information processed by these systems, and on-going efforts to improve security in this area. I have established the protection of intelligence processed by automated systems and networks as one of the Intelligence Community's highest priorities for the 1980s and 1990s. [redacted]

The enclosed assessment was prepared in cooperation with the Department of Defense. ASD(C^3I) provided data concerning military tactical intelligence elements. As you recall, the Senate Appropriations Committee and the House Permanent Select Committee on Intelligence have asked that copies of this assessment be provided to them. Your interest and continued support in this area are appreciated. [redacted]

Sincerely,

John N. McMahon
Acting Director

Enclosure [redacted]

cc: Senate Appropriations Committee
House Permanent Select Committee on Intelligence
Senate Select Committee on Intelligence

[redacted]

[redacted]

STAT

[redacted]

SECURITY IMPLICATIONS OF EXPANDED USE OF COMPUTERS AND AUTOMATED OFFICE EQUIPMENT PROCESSING INTELLIGENCE INFORMATION

BACKGROUND

The Intelligence Community has an enormous investment in computers, networks, and automated office equipment processing intelligence data. [redacted] [redacted]

25X1
STAT

The latest generation of electronic computer and automated office equipment procured by Intelligence Community and DoD intelligence components provides for the storage and processing of a vast amount of information at smart terminals/workstations and personal computers which increasingly are under the control of individual intelligence analysts. Intelligence components reported that three years ago there were approximately 2,000 smart terminals/workstations and personal computers storing intelligence data both on floppy discs and on local hard discs. The average storage capacity of a floppy disc was approximately 30 pages and few local hard discs stored more than 3,500 pages of data. Large volumes of data were available to the intelligence analysts primarily from central computer systems under the centralized control and accountability of data processing organizations. [redacted]

STAT

Today there are over 35,000 smart terminals/workstations and personal computers used by the intelligence components, many having local hard disc storage capacities of up to 2,600 pages per system. Currently, the primary means of storage is the local hard disc with 250 page capacity floppy discs being used as backup storage capabilities. These systems are used to support processing applications such as word processing, graphics, and advanced analytical capabilities. The components estimate that by 1990 there will be over 60,000 terminals and personal computers processing intelligence--some with local hard disc storage capabilities of up to 10,000 pages per system and small removable compact discs that will exceed 1,500 pages of data. The three-inch compact discs are the most difficult to control because of their small size. [redacted]

STAT

ASSESSMENT OF CURRENT RISKS

In late 1983, the DCI began a major review of the Intelligence Community's security posture in the automated information system and data communications network areas as part of his special project on computer security (COMPUSEC). In order to establish priorities for corrective actions, this effort produced

STAT

[redacted]

[redacted]

an all-source assessment of the threat to systems processing intelligence information and included an assessment of the current security status of 13 "critical systems" as a baseline review of the status of all Intelligence Community systems. These actions identified several security vulnerabilities within existing Intelligence Community systems including those related to the use of the equipment highlighted in this report. As a result, the DCI issued new Uniform SAFEGUARDS security requirements for the protection of "Critical Systems" processing intelligence information. The Community continues to support efforts to reduce the risks of processing intelligence information in automated systems and networks in technical, environmental, and administrative security areas. [redacted]

Equipment used by the components is either TEMPEST approved or located within appropriate facilities. [redacted] The sensitivity and increasing volume of information available on these devices dictate that all forms of security be employed to limit the risk of using this equipment while providing the processing capabilities required to satisfy operational needs. [redacted]

CURRENT SECURITY MEASURES

[redacted]

[redacted]

Next 3 Page(s) In Document Denied